## Break

**1:40pm–2:50pm**

***Ed Harrington,* The Open Group**

***Identity Management Work in The Open Group***

The Open Group, together with other bodies, is working for a global identity management framework. Its program started in January 2002, and is ongoing. This presentation will review what has been achieved so far, and describe the current and future projects.

***Joe Donahue,* Microsoft**

***Integration of Directories and Federation***

This will be a discussion of definitions, architectures, the pros and cons of different approaches, and a discussion of where directory technologies like LDAP and DSML relate with existing security standards, like Kerberos, and emerging standards, such as WS-Security, xRML, and SAML.

## Break

**3:00pm–4:25pm**
**Keynote**

***Kevin Mitnick***

***The Art of Deception***

Kevin will share his perspective on the threat of "social engineering"– the highly effective type of attack that exploits the human element of corporate security. Kevin will illustrate why a misplaced reliance on security technologies alone, such as firewalls, authentication devices, encryption, and intrusion detection systems, is virtually ineffective against a motivated attacker using social engineering techniques. Through concrete examples, Kevin will show what your business can do to develop a creative and engaging security program that heightens awareness, motivates employees to change their attitudes, influences them to think defensively, and encourages the adoption of good security habits.

**4:25pm–4:30pm**

***Closing Remarks***

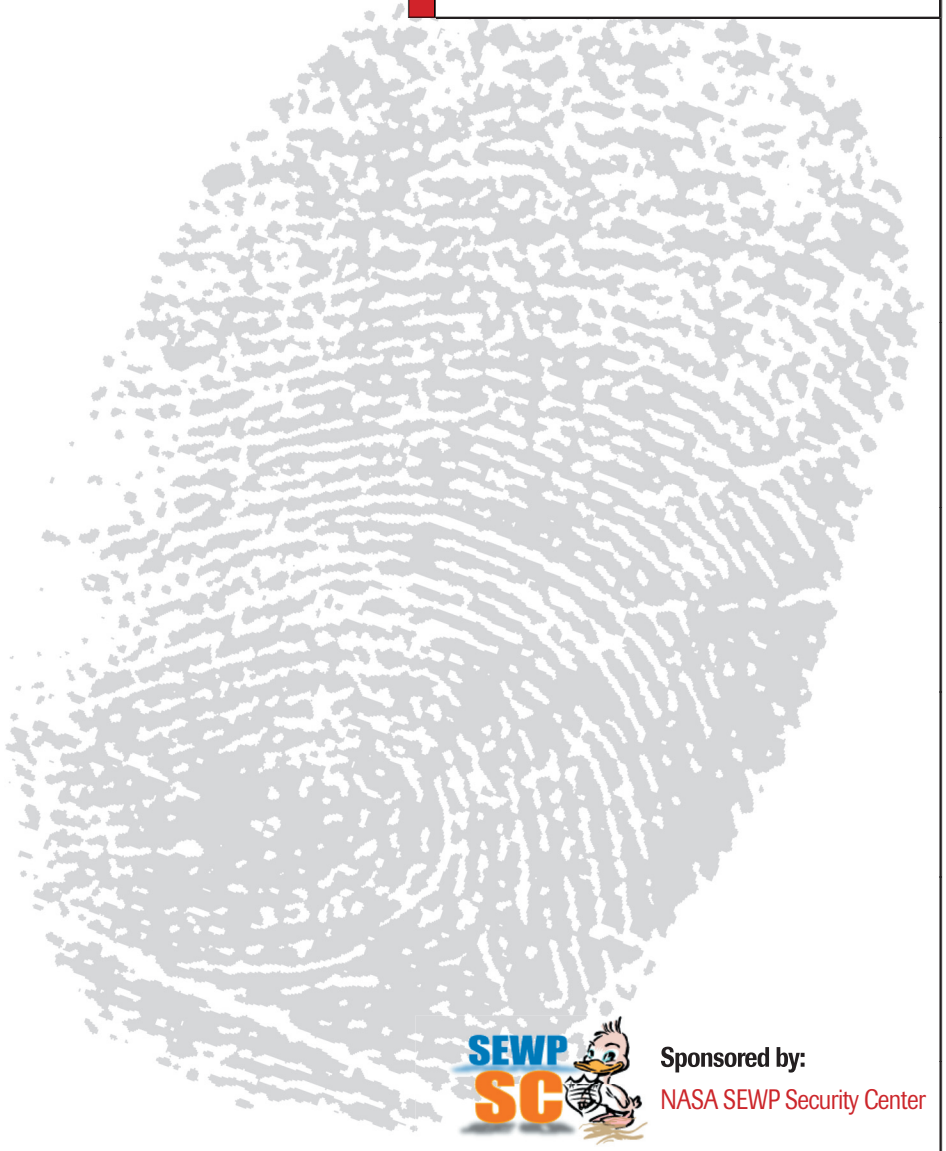
**Sponsored by:**
NASA SEWP Security Center
www.sewpsc.sewp.nasa.gov

NASA SEWP Security Symposium:

# Identity Management

**June 1, 2004**

## Agenda



**Sponsored by:**
NASA SEWP Security Center

## Agenda

**7:45am–8:30am** — ***Registration and Continental Breakfast***

**8:00am–3:30pm** — ***Vendor Exposition***

**8:30am–10:30am**

***Dennis Taylor,* SEWP Security Center**
***Introductory Remarks: The SEWP Security Center***

***Joanne Woytek,* NASA SEWP**
***SEWP III***

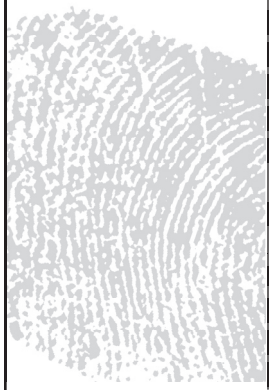
**Keynote**

***Whitfield Diffie,* Sun Microsystems**
***The Prospects for Computer Security***
Attempts to build secure computing environments have been under way with success that is modest by comparison to the original goals. Is there any reason to believe we can do better now? Developments in cryptography, networking, and computer languages suggest that the answer is yes.

***Stephen Whitlock,* Boeing**
***Security Directions at Boeing***
New business requirements, technologies, and threats require new approaches to IT security. This presentation will outline our IT security strategy and give a high level overview of our architectural directions that will be necessary to meet these requirements.

## Break

**10:45am–12:30pm**



***Skip Slone,* Lockheed Martin**
***The Open Group's Identity Management White Paper***
The Open Group's Identity Management work area recently published a white paper on Identity Management. This presentation will provide an overview of the white paper, its major findings, and the "next steps" identified in the paper.

***Steve Ebbets,* Liberty Alliance**
***Liberty Alliance Today and Tomorrow: Business Possibilities and Technical Realities***
Businesses and technology vendors alike have been evangelizing the terms "web services" and "single sign-on" like they're the second coming. But is all the hype really achievable? A number of companies are betting their business on it and are working together to develop what they see as the foundation for these terms. In this session, a technical representative from the Liberty Alliance, a consortium of 150 worldwide for-profit, not-for-profit, and government organizations formed to develop an open, interoperable network identity standard, will address the business benefits of federated identity and implementation and technical considerations for making the hype happen. From a technical standpoint, we'll examine the work of the Liberty Alliance to date and also give a glimpse into what is to come.

***Tim Polk,* NIST**
***NIST E-Authentication Guidance: SP 800-63***
NIST SP 800-63 is focused on the remote authentication of people over a network. This guidance defines technical requirements for remote authentication at four levels of assurance. The technical requirements address identity proofing, token strength, authentication mechanisms, and assertions. SP 800-63 supports agency implementation of the recent OMB guidance "E–Authentication Guidance for Federal Agencies."

## Break / Lunch (working lunch)

**12:45pm–1:30pm**

***Hal Lockhart,* OASIS**
***The XACML Standard for Access Control Policy and Distributed Authorization***
The eXtensible Access Control Markup Language (XACML) is an OASIS standard for expressing and evaluating Authorization Policies. It is designed to provide a very high degree of flexibility and contains features designed to make it suitable for very large–scale, federated environments. This talk will provide an overview of distributed Authorization including other standards such as SAML and where XACML fits. It will provide a summary of the technical features of the XACML, including what is new in version 2.0 and a brief history of the development of SAML, XACML, and related specifications, as well as their current status.